(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 March 2001 (15.03.2001)

PCT

(10) International Publication Number
WO 01/18807 A2

(51) International Patent Classification[7]: G11B 20/00, G06F 1/00, H04L 9/08

(21) International Application Number: PCT/EP00/08054

(22) International Filing Date: 16 August 2000 (16.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/389,825 3 September 1999 (03.09.1999) US

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor: EPSTEIN, Michael, A.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: HOEKSTRA, Jelle; Internationaal Octrooibureau B.V., Prof Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States *(national)*: CN, JP, KR.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/18807 A2

(54) Title: RECOVERY OF A MASTER KEY FROM RECORDED PUBLISHED MATERIAL

(57) Abstract: An encryption of a master key is included with each recording of encrypted published material that requires the master key for decryption and subsequent processing. The master key is encrypted using a public key associated with a trusted authority, typically encoded on a smartcard that is associated with each authorized user. Should the smartcard be lost, or the decryption device become inoperative, one of the recordings containing the encrypted master key is sent to the trusted authority for a retrieval of the master key. The trusted authority uses the private key corresponding to the public key that was used to encrypt the master key to determine the master key. In a preferred embodiment, the trusted authority is the vendor of the smartcard or other encryption/decryption device, and provides a replacement smartcard or device containing the retrieved master key, typically for a fee, for subsequent use by the user to decrypt other recorded material in the user's collection.

Recovery of a master key from recorded published material

This invention relates to the field of consumer electronics, and in particular to the recovery of published material that is recorded in an encrypted form.

Digital recordings have the unique property that copies of the content material have the same quality as the original. As such, the need for an effective copy protection scheme is particularly crucial for the protection of content material that is digitally recorded. A number of protection schemes have been developed or proposed that record the content material in an encrypted form. Other protection schemes have been developed or proposed that record an encrypted key that controls the playback, or rendering, of the content material. In a number of these schemes, a "smartcard" is used to decrypt the encrypted information. The smartcard contains a master key that is used to encrypt and decrypt the content material or to encrypt or decrypt another key that controls the rendering of the content material. Alternatively, the master key is contained within the recording or playback device, or within a content-access-module that is used to decrypt the content material. A smartcard or content-access-module is typically preferred, so as to allow the use of alternative or replacement recording or playback devices.

After some time, the user will accumulate a collection of recordings that contain content material that can only be accessed via the use of the smartcard containing the master key. In this encrypted environment, a loss of the smartcard, or a failure of the content-access-module will effectively render the user's collection of recordings virtually worthless. Other encrypted collections, such as computer file systems, are also equally vulnerable to the loss of an access device or master key. A conventional method for alleviating the inconvenience and impact associated with the loss of a smartcard is to maintain a registry of each smartcard and its associated master key. Such a system, however, requires that the user have a means for identifying the particular smartcard after it is lost, or requires that the registry contain an identification of each user of each smartcard. Such a system is difficult to administer, and prone to administrative mishaps that could result in the complete loss of the user's collection due to a misregistration or erroneous identification of the user.

In the field of law enforcement and national security, "digital lockbox" techniques have been proposed for providing emergency access to encrypted files by encrypting the master key using a public key of a trusted authority, and including the encryption of the master key with each encrypted file. U.S. Patents 5,557,346 and 5,557,765, and PCT publications WO 99/04530 and WO 98/47260 discuss these techniques, and are incorporated by reference herein. The techniques presented in these publications, however, are encumbered with various safeguards to prevent the unauthorized access to the encrypted information, to protect the privacy of the individual who created the information.

In the field of consumer electronics, different considerations from law enforcement are relevant. The content material is intended to be published for use by the general public. This published material is encrypted to prevent it from being copied or used by persons other than those who have acquired the right to access the published material, and those who have acquired the right to access the material have no privacy rights or concerns regarding access to the material. In effect, the encryption process inconveniences those who have acquired the right to access the published material. The success of imposing the proposed encryption schemes for safeguarding copy protected published material will be highly dependent on the general public's acceptance of this inconvenience, and in particular, to any loss of value incurred due to a misplaced or defective decryption device.

It is an object of this invention to provide a method and device for recording encrypted published material that facilitates a simple retrieval of a master key that can be used to decrypt the published material. It is a further object of this invention to provide a method of providing a replacement decryption device that contains a master key that is suitable for decrypting encrypted information.

This objective and others are achieved by including an encryption of a master key with each recording that contains encrypted published material that requires the master key for decryption and subsequent processing. The master key is encrypted using a public key associated with a trusted authority. Should the smartcard be lost, or the decryption device become inoperative, any one of the recordings containing the encrypted master key is sent to the trusted authority for a retrieval of the master key. The trusted authority uses the private key corresponding to the public key that was used to encrypt the master key to determine the master key. In a preferred embodiment, the trusted authority is the vendor of the smartcard or other encryption/decryption device, and provides a replacement smartcard or device

containing the retrieved master key, typically for a fee, for subsequent use by the user to decrypt other recorded material in the user's collection.

The invention is explained in further detail, and by way of example, with reference to the accompanying drawings wherein:

FIG. 1 illustrates an example block diagram of a system for recording encrypted published material in accordance with this invention.

FIG. 2 illustrates an example flow diagram of a system for recording encrypted published material in accordance with this invention.

FIG. 3 illustrates an example flow diagram for the retrieval of a master key in accordance with this invention.

Throughout the drawings, same reference numerals indicate similar or corresponding features or functions.

FIG. 1 illustrates an example block diagram of a system 100 for recording encrypted published material, such as audio content, audio-visual content, virtual-reality content, multi-media content, and the like, in accordance with this invention. For the purposes of this specification, the term published material is used in the general sense of content material that is recorded by one party for distribution to other parties, typically the general public. That is, the encryption of the material is not to preserve the secrecy of the content material, but rather to preserve the copy and viewing rights to the published material.

An encryption device 110 receives the content material 101 and provides encrypted material to a recording device 130 for recording onto a medium 140. As is common in the art, the content material 101 is often communicated from a source, such as a "pay-per-view" broadcaster, in encrypted form and decrypted locally. For ease of understanding, this decryption stage is not illustrated in FIG. 1 and is not discussed further in this disclosure.

Depending upon the specific standard or convention employed by the encryption device 110, the encryption device 110 encrypts the content material using either a master key M 121 to produce an encryption $E_M(CM)$ 112, or a session key K to produce an encryption $E_K(CM)$ 114. The master key M 121 is intended to remain constant for all encryptions of the particular system 100, and is commonly provided by, for example, a

smartcard, illustrated in FIG. 1 as an access device 120. Alternatively, the access device 120 may be embodied within a separate access module, such as a set-top-box or other device. As is common in the art, the session key K may change for each particular content material, or each content material classification, and may contain, for example, a ticket or other item that identifies the display or copy rights to the content material. Copending U.S. Patent Application "Copy Protection by Ticket Encryption", serial number 09/333,628, filed 6/15/99 for Michael Epstein, Attorney docket PHA 23,457, presents techniques for copy and display protection of copyright material, and is incorporated by reference herein. The session key K is commonly generated locally, using, for example, a key-exchange between the encryption device 110, and a corresponding decryption device 160. Copending U.S. Patent Application "Key Exchange Via a Portable Remote Control Device", serial number _____, filed _____ for Michael Epstein, Attorney docket PHA _____(Disclosure 700621), presents methods and applications for exchanging cryptography keys between authorized devices, and is incorporated by reference herein.

In accordance with this invention, the access device 120 that provides the master key M 121 also provides a public key P 122 that is associated with a trusted authority, such as the vendor of the access device 120. The public key P 122 is part of a public-private key-pair, the private key of the key-pair being a secret kept at the trusted authority. An item that is encrypted using the public key of the key-pair can only feasibly be decrypted by the private key of the key-pair. The encryption device 110 encrypts the master key M 121 using the public key P 122, and communicates the encrypted master key $E_P(M)$ 111 to the recording device 130 for inclusion on the medium 140 with the encrypted content material $E_M(CM)$ 112 or $E_K(CM)$ 114. If the encrypted content material is encoded using the session key K, the encryption device 110 also encrypts the session key K using the master key M, and provides an encrypted session key $E_M(K)$ 113 to the recording device 130 for inclusion on the medium 140 as well. In many cases, it is difficult to store a session key K on a smartcard, whereas the inclusion of an encryption of the session key based on a master key M 121 provides a means for retrieving the session key K via the use of a smartcard containing the master key M 121. Note that by encrypting the content material CM 101 or the key K to decrypt the encrypted content material $E_K(CM)$ 114 using the master key M 121, and storing these encryptions 111, 112 or 111, 113, 114 on the medium 100, the content material CM 101 can be recovered by a decryption, or series of decryptions, based on the master key M 121.

To render the encrypted content material that is stored on the medium 140, a playback device 150 communicates the encrypted material 111, 112 or 111, 113, 114 from

the medium 140 to the decryption device 160. The medium 140 may be any of a variety of recording mediums including magnetic tape, magnetic disks, laser disks, CDs, DVDs, and so on. The playback device 150 is a corresponding device for reading the material on the medium. If the medium 140 is a hard disk drive, for example, the playback device 150 may be a computer system that reads files that are stored on a hard disk drive. The decryption device 160 can receive the master key from the access device 120, if required. If the content material CM 101 is encrypted using the session key K, as $E_K(CM)$ 114, and the decryption device 160 is privy to the session key K, it does not need the master key M 121 to decrypt a copy 101' of the content material CM 101. If, on the other hand, the decryption device 160 does not have direct access to session key K, or the content material CM 101 is encrypted using the master key M 121, as $E_M(CM)$ 112, the decryption device 160 receives the master key M 121 from the access device 120 and provides thereafter a copy 101' of the content material CM 101. This copy 101' of the content material CM 101 is provided to a conventional rendering device 170 for presentation to the user in a suitable form. For example, if the content material CM 101 is an audio recording, the rendering device 170 provides an audio representation of the content material CM 101. Similarly, if the content material CM 101 is a plurality of stimuli associated with a virtual reality environment, the rendering device 170 provides the appropriate representations of each of the recorded stimuli.

FIG. 2 illustrates an example flow diagram for recording encrypted content material in accordance with this invention, as may be effected by the encryption device 110 of FIG. 1. For ease of understanding, the use of a session key K, and the encryption of the session key K using the master key M, is not illustrated in FIG. 2; the details for adding this option will be evident to one of ordinary skill in the art in view of this disclosure. The process commences upon receipt of the content material CM, at 210. Thereafter, the encryption device 110 receives a master key M and a public key P, at 220, typically from an access device 120 in FIG. 1. The encryption device 110 encrypts the master key M using the public key P, at 230, and records the encrypted master key $E_P(M)$, at 240. The content material is encrypted, at 250, using the master key M, and the encrypted content material $E_M(CM)$ is similarly recorded, at 260. In accordance with this invention, the recording of the encrypted master key $E_P(M)$ and the encrypted content material $E_M(CM)$ is preferably stored on the same medium 140.

As can be seen from the above, a knowledge of the master key M allows for the decryption of all material that is recorded in accordance with this invention.

FIG. 3 illustrates an example flow diagram for the retrieval of a master key M in accordance with this invention. FIG. 3 illustrates example actions that occur at a provider's locale and at a user's locale. At 310, the provider provides a master key M and a public key P to the user, the master key M and public key P being typically provided on a smartcard that is used to facilitate the encryption of copy-protected material via a conforming system 350. Alternatively, the master key M may be generated randomly on the smart card, and not known to the provider. As noted above, a number of standards have been proposed that call for the encryption of copy-protected material using a master key M that is unique for each user, to prevent the uncontrolled reproduction of copy-protected content material CM. A conforming system 350 effects and enforces the encryption and copy protection in accordance with these standards. Via the conforming system 350 that includes encryption, decryption, recording, and playback capabilities, the user is able to create a collection 360 of encrypted content material CM that conforms to the appropriate standards, and is able to decrypt and playback the encrypted content material CM, via the use of the provided master key M.

If the user loses the master key M, or the smartcard becomes faulty, the provider provides the user with a replacement master key M, via the following process, illustrated in FIG. 3. The user selects an individual encrypted recording 361 from the collection 360 and sends it to the provider. In lieu of sending the original encrypted recording 361, a copy of the recording 361 can be sent, provided that the copy contains an unmodified copy of the encrypted master key $E_P(M)$. The provider decrypts the encrypted master key $E_P(M)$, using the corresponding private key p, at 320, and provides a replacement copy of the master key M and public key K, at 330, typically by sending the user a replacement smartcard in return for a servicing fee. In this manner, by paying the associated service fees, a user is able to continue to access and playback each recording of the user's collection 360.

FIG. 4 illustrates an example block diagram of a system for providing a replacement access device 120' in accordance with this invention. The playback device 410 accesses the encrypted recording 361 from the user's collection 360 of FIG. 3 to provide the encrypted master key $E_P(M)$ to a decryption device 420. The decryption device 420 uses the private key p 401 to decrypt the encrypted master key $E_P(M)$ to provide the master key M. A programming device loads the decrypted master key M, and the public key P corresponding to the private key p 401 into the duplicate access device 120' that is sent back to the user, typically with the encrypted recording 361.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the invention and are thus within its spirit and scope. For example, controls may be incorporated into the process illustrated in FIG. 3 to assure that the number of copies of the master key M is limited. For example, a simple record of the number of times a master key M is provided can be maintained, and further copies of the master key M may be precluded. Alternatively, providing each copy of the master key M can have an increasingly higher fee charged, or some other procedure employed, so as to make an unauthorized mass distribution of the same master key M economically infeasible, or highly inefficient.

The particular structures and functions of the figures in this disclosure are presented for illustration purposes. Other configurations and functional implementations are feasible. For example, the access device 120 may be a programmable device that is downloaded with a master key M upon activation. Thereafter, the aforementioned process of replacing the access device 120 may include the downloading of a copy of the master key M, based on a transmission of encrypted master key $E_P(M)$ to the downloading entity. These and other system configuration and optimization features will be evident to one of ordinary skill in the art in view of this disclosure, and are included within the scope of the following claims.

CLAIMS:

1. A method for recording published material (101) comprising:
encrypting (210) the published material (101) to produce an encrypted content (112, 114) that depends upon a master key (121) to facilitate a decryption of the encrypted content (112, 114), encrypting (230) the master key (121) to produce an encrypted master key (111) that depends upon a private key (p) to facilitate a decryption of the master key (121), recording (240) the encrypted master key (111) and the encrypted content (112, 114) on a recording medium (140).

2. The method of claim 1, wherein
encrypting (210) the published material (101) includes:
encrypting the published material (101) using a first key (K) to produce the encrypted content (114),
encrypting the first key (K) to produce an encrypted first key (113) that depends upon the master key (121) to facilitate a decryption of the first key(K), and the method further includes:
recording the encrypted first key (113) on the recording medium (140).

3. The method of claim 1, wherein the encrypting (230) of the master key (121) is based on a public key (P) that corresponds to the private key (p) as a public-private key pair.

4. The method of claim 1, wherein the published material (101) comprises at least one of: audio material, video material, audio-visual material, and virtual reality material.

5. The method of claim 1, wherein the recording medium (140) is at least one of: a magnetic tape, a magnetic disk, a laser disk, a CD, and a DVD.

6. A method of providing a replacement access device (120') for facilitating a decryption of an encrypted content material (112, 114) comprising:

receiving a recording (361) from a user that includes an encryption (111) of a master key (121) based on a public key (P), decrypting (320) the encryption (111) of the master key (121) to produce a copy of the master key (121), using a private key (p) that corresponds to the public key (P) as a public-private key pair, encoding (430) the copy of the master key (121) in the replacement access device (120'), and providing (330) the replacement access device (120') to the user.

7. The method of claim 6, further including:
providing an original access device (120) that contains the master key (121) to the user.

8. The method of claim 6, further including:
maintaining a record of each copy of the master key (121), and providing (330) the replacement access device (120') in dependence upon the record.

9. The method of claim 6, further including:
assessing a fee for providing the replacement access device (120').

10. The method of claim 9, further including:
maintaining a record of each copy of the master key (121), and determining the fee for providing the replacement access device (120') in dependence upon the record.

11. The method of claim 10, wherein
determining the fee includes:
determining a number of occurrences of each copy of the master key (121), and determining the fee in correlation with the number of occurrences.

12. The method of claim 6, wherein the recording (361) is contained on at least one of: a magnetic tape, a magnetic disk, a laser disk, a CD, and a DVD.

13. A system comprising:
an encryption device (110) that is configured to:
encrypt published material (101) to provide encrypted content material (112, 114) whose decryption depends upon a master key (121), and encrypt the master key (121) to provide an encrypted master key (111) whose decryption depends upon a private key (p), and a

recording device (130) that is configured to record the encrypted master key (111) and the encrypted content material (112, 114) on a recording medium (140).

14. The system of claim 13, wherein the recording medium (140) is at least one of: a magnetic tape, a magnetic disk, a laser disk, a CD, and a DVD.

15. The system of claim 13, wherein the encryption device (110) is configured to encrypt the master key (121) based on a public key (P) that corresponds to the private key (p) as a public-private key pair.

16. The system of claim 13, wherein the encryption device (110) is configured to encrypt the published material such that:
the published material (101) is encrypted via a first key (K) to produce the encrypted content material (114), and the first key (K) is encrypted via the master key (121) to produce an encrypted first key (113), and, the recording device (130) is further configured to record the encrypted first key (113).

17. A system for providing a replacement access device (120') comprising:
a playback device (410) that provides an encrypted master key (111) from a recording (361) that contains an encrypted master key (111) based on a public key (P) of a public-private key pair and encrypted content material (112, 114) that is decryptable based on a master key (121) corresponding to the encrypted master key (111), a decryption device (420) that decrypts the master key (121) from the encrypted master key (111) based on a private key (p) that corresponds to the public key (P) of the public-private key pair, a programming device (430) that records the master key (121) on the replacement access device (120').

18. The system of claim 17, wherein the programming device (430) also records the public key (P) on the replacement access device (120').

19. A recording (361) contained on a medium comprising:
an encryption (111) of a master key (121) based on a public key (P) of a public-private key-pair whose decryption is facilitated by a private key (p) of the public-private key-pair, and an encryption of published material (101) whose decryption is facilitated by the master key (121).

20. The recording (361) of claim 19, wherein the medium includes at least one of: a magnetic tape, a magnetic disk, a laser disk, a CD, and a DVD.

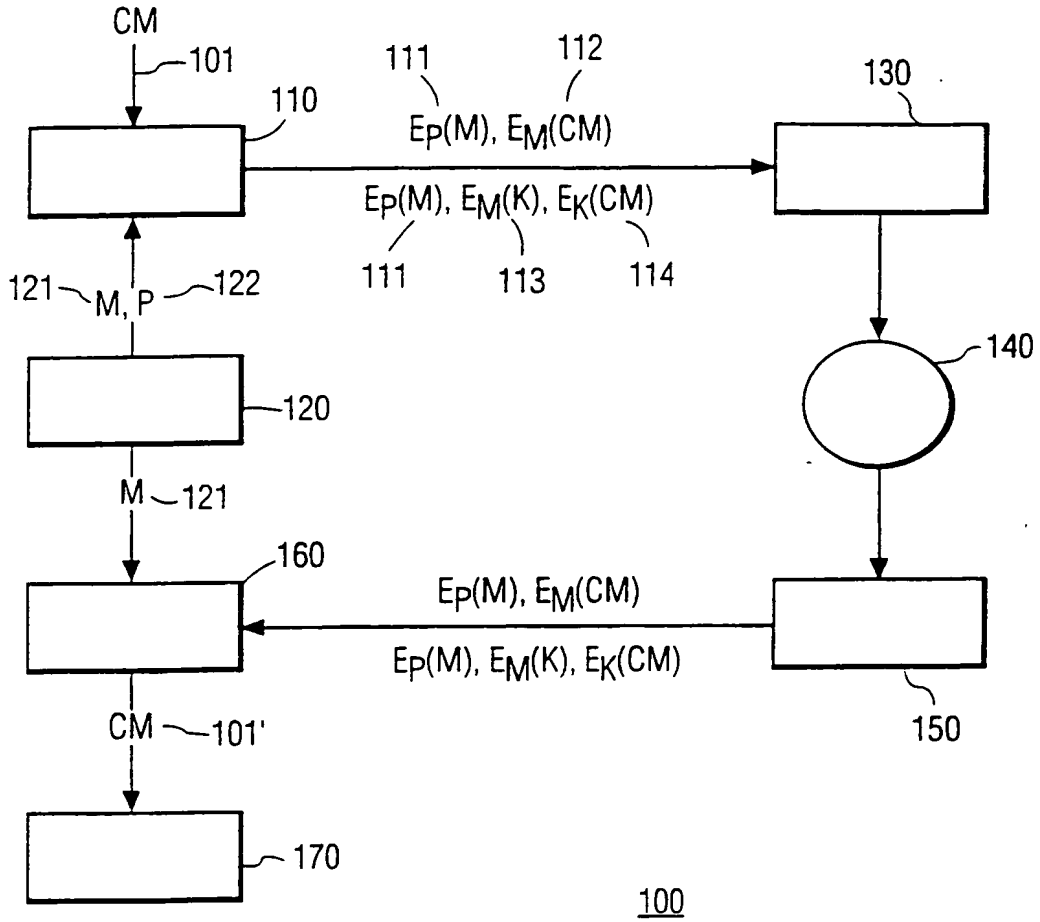

CM
101
110
111
112
$E_P(M)$, $E_M(CM)$
130
$E_P(M)$, $E_M(K)$, $E_K(CM)$
111
113
114
121
M, P
122
140
120
M
121
160
$E_P(M)$, $E_M(CM)$
$E_P(M)$, $E_M(K)$, $E_K(CM)$
CM
101'
150
170
100

FIG. 1

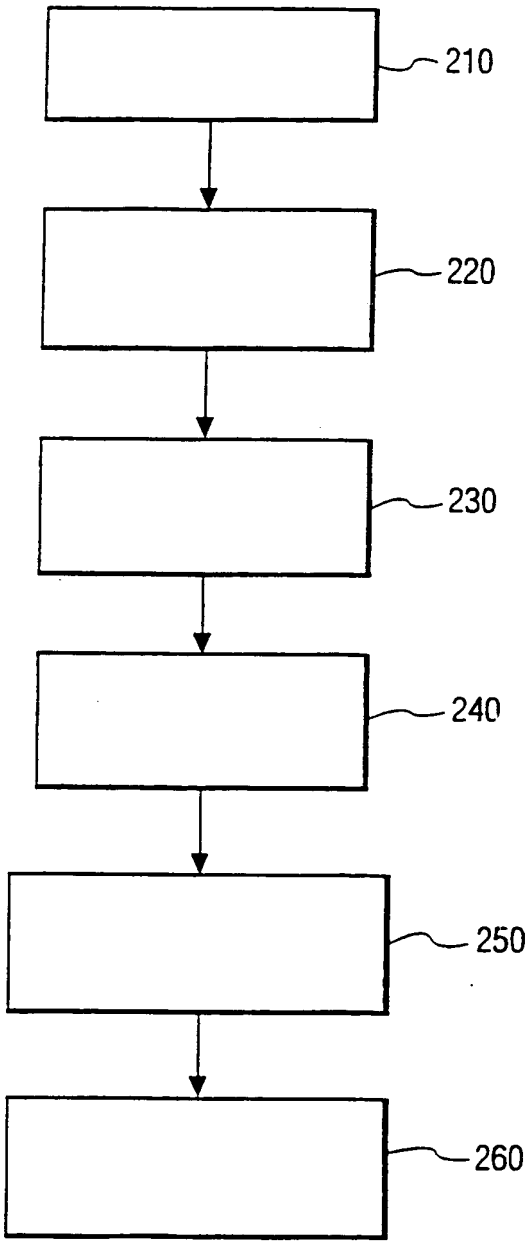


FIG. 2

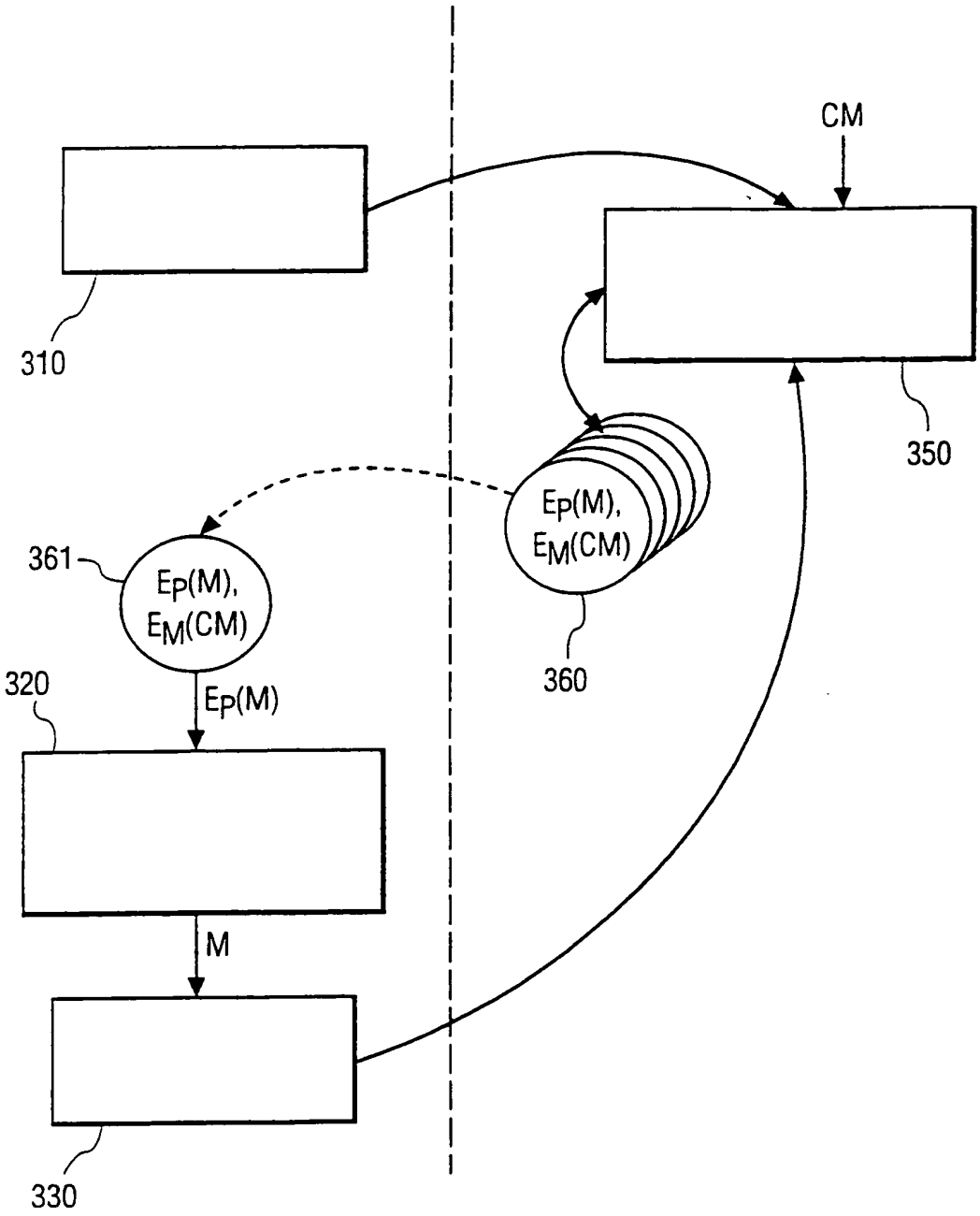


FIG. 3

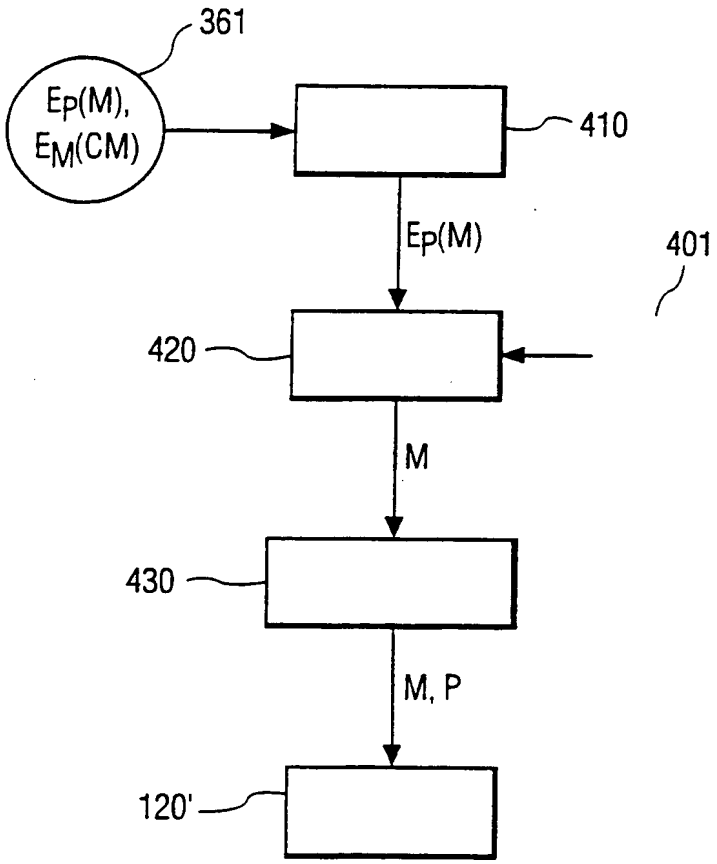


FIG. 4

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 March 2001 (15.03.2001)

PCT

(10) International Publication Number
WO 01/18807 A3

(51) International Patent Classification[7]: G11B 20/00, G06F 1/00, H04L 9/08

(21) International Application Number: PCT/EP00/08054

(22) International Filing Date: 16 August 2000 (16.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/389,825 3 September 1999 (03.09.1999) US

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor: EPSTEIN, Michael, A.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: HOEKSTRA, Jelle; Internationaal Octrooibureau B.V., Prof Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States *(national)*: CN, JP, KR.

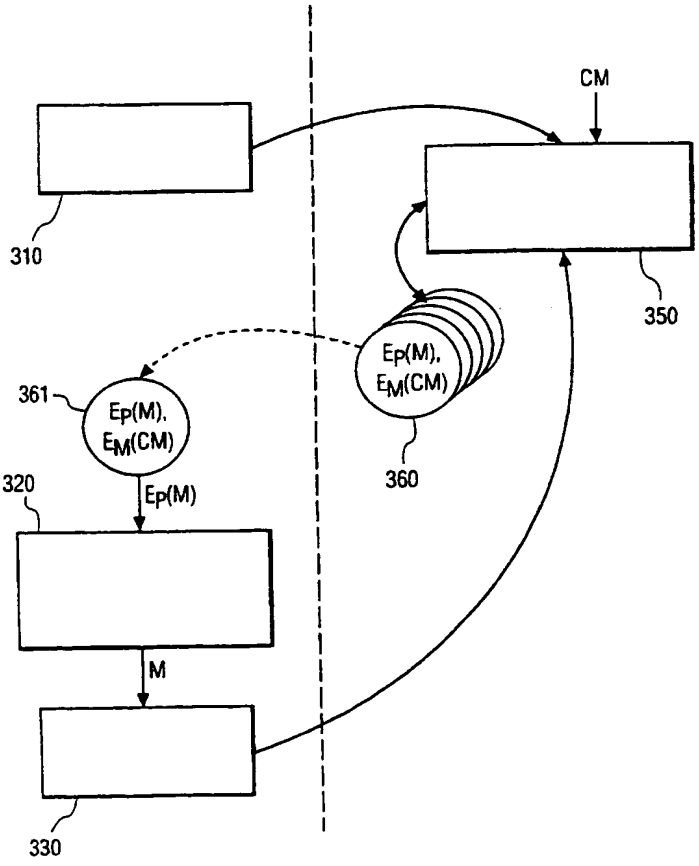
(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *with international search report*

(88) Date of publication of the international search report:
4 October 2001

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: RECOVERY OF A MASTER KEY FROM RECORDED PUBLISHED MATERIAL



(57) Abstract: An encryption of a master key is included with each recording of encrypted published material that requires the master key for decryption and subsequent processing. The master key is encrypted using a public key associated with a trusted authority, typically encoded on a smartcard that is associated with each authorized user. Should the smartcard be lost, or the decryption device become inoperative, one of the recordings containing the encrypted master key is sent to the trusted authority for a retrieval of the master key. The trusted authority uses the private key corresponding to the public key that was used to encrypt the master key to determine the master key. In a preferred embodiment, the trusted authority is the vendor of the smartcard or other encryption/decryption device, and provides a replacement smartcard or device containing the retrieved master key, typically for a fee, for subsequent use by the user to decrypt other recorded material in the user's collection.

WO 01/18807 A3

INTERNATIONAL SEARCH REPORT

Inte tional Application No
PCI/EP 00/08054

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 G06F1/00 H04L9/08'

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B G06F H04L G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99 04530 A (V ONE CORP) 28 January 1999 (1999-01-28) cited in the application figure 1 page 2, line 10 - line 15 page 11, line 13 - line 21 page 13, line 15 - line 24	1,3-5, 13-15, 19,20
Y	page 15, line 14 -page 16, line 4	6,7,9, 12,17
A	---	2,16
Y	EP 0 679 029 A (SCIENTIFIC ATLANTA) 25 October 1995 (1995-10-25) page 2, line 33 - line 38 page 5, line 6 - line 34 page 13, line 8 - line 11	6,7,9, 12,17
A	figures 7,8	18

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 March 2001	20. 03. 2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ogor, M

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 00/08054

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No
X	EP 0 773 490 A (FUJITSU LTD) 14 May 1997 (1997-05-14) figure 9 column 2, line 16 - line 27	1,4,5, 13,14
A	column 3, line 40 - line 44	19,20
X	EP 0 802 535 A (MATSUSHITA ELECTRIC IND CO LTD) 22 October 1997 (1997-10-22) page 1, line 11 - line 20 page 12, line 58 -page 13, line 38 figure 13	1,2,4,5, 13,14,16
E	WO 00 62290 A (KONINKL PHILIPS ELECTRONICS NV) 19 October 2000 (2000-10-19) the whole document	1,3-5, 13-15, 19,20
A	EP 0 936 812 A (CANAL PLUS SA) 18 August 1999 (1999-08-18) column 2, line 20 - line 50 column 3, line 26 - line 41 column 4, line 11 - line 28 column 13, line 34 -column 14, line 21 column 18, line 49 - line 55	1,4-7, 12-14, 17,19,20
A	TASKETT J: "SMART CARDS AS A REPLACEABLE SECURITY ELEMENT FOR TELEVISION DELIVERY ACCESS CONTROL" PROCEEDINGS OF THE ANNUAL CONVENTION AND EXPOSITION,US,WASHINGTON, NCTA; vol. CONVENTION 42, 6 June 1993 (1993-06-06), pages 128-132, XP000410492	

2

INTERNATIONAL SEARCH REPORT

rnational application No.
PCT/EP 00/08054

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-5 13-16 19-20

   System for recording encrypted published material that facilitates simple retrieval of a locally generated session key that can be used to decrypt the published material.

2. Claims: 6-12 17-18

   Providing a replacement decryption device (e.g a smart card) that contains a key suitable for decrypting encrypted information, in case the original device is lost or becomes inoperative.

INTERNATIONAL SEARCH REPORT

Inte ional Application No
PCT/EP 00/08054

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9904530 A	28-01-1999	AU 8757398 A	10-02-1999
EP 0679029 A	25-10-1995	US 5237610 A	17-08-1993
		EP 0683614 A	22-11-1995
		AT 144670 T	15-11-1996
		AT 181196 T	15-06-1999
		AT 180373 T	15-06-1999
		AU 650958 B	07-07-1994
		AU 1384092 A	01-10-1992
		BR 9201106 A	24-11-1992
		CN 1066950 A,B	09-12-1992
		DE 69214698 D	28-11-1996
		DE 69214698 T	06-03-1997
		DE 69229235 D	24-06-1999
		DE 69229235 T	23-09-1999
		DE 69229408 D	15-07-1999
		DE 69229408 T	11-11-1999
		EP 0506435 A	30-09-1992
		JP 5145923 A	11-06-1993
		SG 44801 A	19-12-1997
EP 0773490 A	14-05-1997	JP 9134311 A	20-05-1997
		JP 9134330 A	20-05-1997
		US 5857021 A	05-01-1999
EP 0802535 A	22-10-1997	WO 9714147 A	17-04-1997
WO 0062290 A	19-10-2000	BR 0005458 A	30-01-2001
EP 0936812 A	18-08-1999	EP 0936774 A	18-08-1999
		AU 2295199 A	30-08-1999
		BR 9907878 A	31-10-2000
		EP 1057332 A	06-12-2000
		HR 20000487 A	28-02-2001
		WO 9941907 A	19-08-1999
		NO 20004063 A	13-10-2000
		AU 2296499 A	30-08-1999
		BR 9907877 A	31-10-2000
		EP 1055305 A	29-11-2000
		HR 20000486 A	28-02-2001
		WO 9941874 A	19-08-1999
		NO 20004062 A	13-10-2000